REMARKS

The Office Action mailed April 22, 2004 has been received and reviewed. Claims 1-59 are in the case. Claims 1-5, 8, 13-16, 26-28, 30, 33, 35-37, 42-45, 48-52, and 56-58, and also claims 29, 47, and 53-55, stand rejected under 35 U.S.C. 102(e) as being anticipated by Vanstone et al. (hereinafter referred to as Vanstone) (U.S. Patent No. 6,141,420). Claims 6, 7, 9-12, 17-25, 31, 32, and 59, and also claims 34 and 46, stand rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone. Claims 38-41 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone in view of Elkies (Reference V).

By this paper, Applicant has amended claims 1, 26, and 29 to more particularly point out and distinctly claim the novel and nonobvious subject matter of the invention. For the reasons set forth below, claims 1-59 are believed to be in condition for immediate allowance. Favorable reconsideration of the application in view of the following remarks, is therefore respectfully requested.

REJECTION OF CLAIMS 1-5, 8, 13-16, 26-28, 29, 30, 33, 35-37, 42-45, 47, 48-52, 53-55 and 56-58, UNDER 35 U.S.C. 102(E), OVER VANSTONE

Claims 1-5, 8, 13-16, 26-28, 29, 30, 33, 35-37, 42-45, 47, 48-52, 53-55, and 56-58 stand rejected under 35 U.S.C. 102(e), as being anticipated by Vanstone.

Independent claims 1, 26, and 29 have been amended to recite that "the point modification algorithm includes at least one occurrence of point fractioning". Applicant does not find point fractioning disclosed in Vanstone. Vanstone teaches multiplication of an elliptic curve point by a whole number: He illustrates the calculation of multiples of a point P by adding together combinations such as P+P to give 2P, and by using these combinations in further additions such as 2P+2P to give 4P, and 4P+P to give 5P. The only results obtainable by such methods are whole number multiples of the point P. He does not consider non-integer multiples of an elliptic curve point, such as point fractioning or halving, or imaginary or complex multiplication. Vanstone does mention (column 10, line 61) an operation for rotating a finite field element in his arithmetic unit, but this is insufficient for calculating any multiple of an elliptic curve point, let alone a fractional multiple. Simply multiplying point

coordinates by a number or a field element will not produce resulting points on the same elliptic curve.

The amended claims 1, 26, and 29, include an element (point fractioning) not contemplated in Vanstone, and are not anticipated by Vanstone. In view of the foregoing, Applicant respectfully submits that independent claims 1, 26, and 29, as amended, distinguish over the cited art. Claims 2-5, 8, 13-16, 36-37, 42-45, 47, 48-52, 53-55, and 56-58 depend directly or indirectly on claim 1 as amended, and are therefore distinguished over Vanstone. Claims 27 and 28 depend on claim 26 as amended, and are therefore distinguished over Vanstone. Claims 30, 33, and 35 depend on claim 29 as amended, and are therefore distinguished over Vanstone.

Accordingly, Applicant requests that the Examiner withdraw the rejections of claims 1-5, 8, 13-16, 26-28, 29, 30, 33, 35-37, 42-45, 47, 48-52, 53-55, and 56-58 under 35 U.S.C. 102(e), as being anticipated by Vanstone.

REJECTION OF CLAIMS 6, 7, 9-12, 17-25, 31, 32, 34, 46, and 59, UNDER 35 U.S.C. 103(A), OVER VANSTONE

Claims 6, 7, 9-12, 17-25, 31, 32, 34, 46, and 59, stand rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone.

The Office Action incorrectly asserts (paragraph 27) that Vanstone teaches modification algorithms selected from point multiplication and point fractioning. To the contrary, Vanstone does not teach point fractioning. The rotation operation cited in Vanstone (column 10, line 61) only operates on field elements, not on curve points. Vanstone does not mention point fractioning, or give any way to accomplish it, or suggest that it might be useful.

Claims 1 and 29 have been amended to include point fractioning, which distinguishes them over Vanstone. Claims 6, 7, 9-12, 17-25, and 46 depend directly or indirectly on claim 1 as amended. Claims 31, 32, and 34 depend indirectly on claim 29 as amended.

Consistent with the foregoing, Applicant respectfully requests that the Examiner withdraw the rejections of claims 6, 7, 9-12, 17-25, 31, 32, 34, and 46 under 35 U.S.C. 103(a)

based on Vanstone.

For claim 59, the Office Action states that the claimed steps correspond to the functions of the elements of the method claim 18, which was rejected under 35 U.S.C. 103(a) as unpatentable over Vanstone. In fact, claim 59 recites "the point modification algorithm comprising one or more ambiguous triplication steps, where the ambiguity is resolved by determining whether a point is twice halvable". This element does not occur in claim 18. Moreover, Vanstone does not teach ambiguous triplication steps, nor resolving an ambiguity by determining whether a point is twice halvable. Vanstone does not discuss whether points might or might not be halvable. Applicant submits that claim 59 is distinguished over the cited art.

Accordingly, Applicant respectfully requests that the Examiner withdraw the rejection of claim 59 under 35 U.S.C. 103(a) based on Vanstone. In view of the foregoing, Applicant respectfully asserts that claim 59 is in condition for immediate allowance.

REJECTION OF CLAIMS 38-41 UNDER 35 U.S.C. 103(A), OVER VANSTONE IN VIEW OF ELKIES

Claims 38-41 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone in view of Elkies (Reference V).

Claim 38 recites, in part, "and the finite field is represented as a field tower". The Office Action rejects claim 38 as an obvious combination of Vanstone with Elkies. But Vanstone does not discuss field towers. And Elkies does not discuss field towers either. Elkies discusses towers of modular curves, which are mathematical objects different from the field towers of the present patent application. Moreover, Elkies does not mention any aspect of encryption or concealment of information. Since neither reference suggests the combination of these two elements, the combination cannot be regarded as obvious.

In addition, claim 38 depends on claim 1, as amended to include point fractioning, which is not discussed in either reference. Applicant submits that that claim 38 is distinguished over the combination of cited arts. Claims 39-41 depend on claim 38.

Accordingly, applicant respectfully requests that the examiner withdraw the rejection of claims 38-41 under 35 U.S.C. 103(a) based on Vanstone in view of Elkies.

CONCLUSION

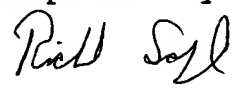
By this paper, claims 1, 26, and 29 have been amended to more fully distinguish the invention. Claims 2-25, 27, 28, and 30-58 are dependent upon claims 1, 26, and 29.

Applicant respectfully requests reconsideration of claims 1-58, as amended, and reconsideration of claim 59.

In the event the examiner finds any remaining impediment to the prompt allowance of any of these claims, which could be clarified in a telephone conference, the examiner is respectfully urged to initiate the same with the undersigned.

DATED this 22nd day of October, 2004.

Respectfully submitted,



Richard Schroeppel, Applicant
500 S. Maple Drive
Woodland Hills, Utah 84653
Telephone: 801-423-7998
Date: October 22, 2004